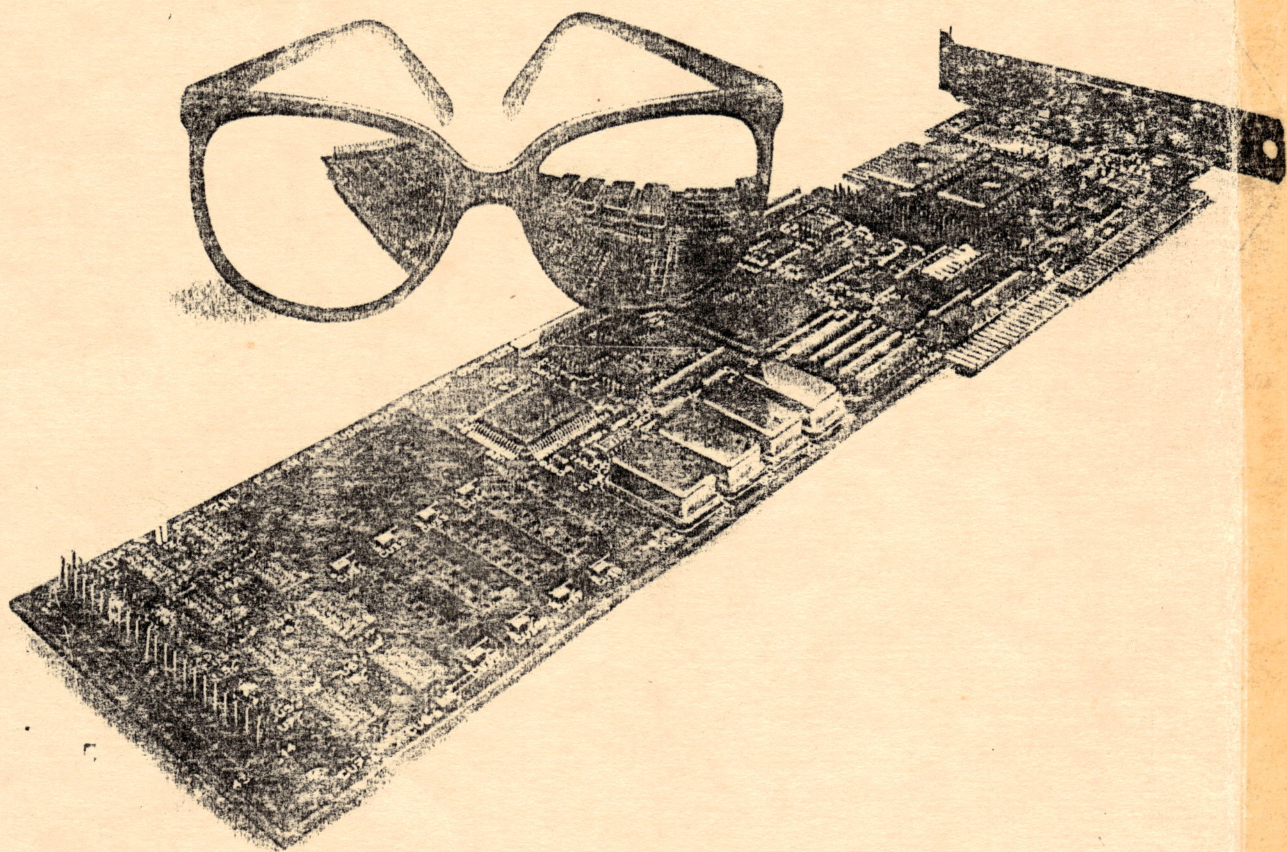
נגיפי מחשב



מ ו ג ב ל

ת ו כ ן ע נ י נ י ם

הקדמה

נגיפי המחשבים למיניהם, הדביקו ומדביקים אלפי מחשבים ותוכנות, תוך גרימת נזק רב. ולכן, חובה על כל משתמש, תוכניתן, או המשתמש המקצועי להכיר את ה"תסמונת הנגיפית", ואת הדרכים להמנע מנזקיהם.

חוברת זו תסייע לך להבין את הבעייה, להכיר את דרכי ההתמודדות ולהערך לעתיד כדי להמנע מנזקים. בחוברת זו נסקרים בקצרה תכונות הנגיפים השונים, הסימנים לפיהם ניתן לאתר הדבקה, סוגי הנגיפים והדרכים היעילות (המוכרות) להתגוננות בפניהם.

הסקירה מטפלת בנגיפים התוקפים מערכות MS-DOS ו"מקינטוש". יודגש כי מאמר זה אינו מתיימר לסקור את כל סוגי הנגיפים, ולהציע פתרונות לכל בעיה נגיפית העלולה להתעורר, מטרתה העיקרית היא, בהפניית תשומת לב המשתמש לבעיה ולדרכי ההתגוננות מפניה.

פרק 1

מהו נגיף המחשב

נגיפי המחשבים הינם תוכניות המשכפלות עצמן לתוך קבצים המורצים במערכת. הם מצמידים עצמם כך שיוכלו לקחת את הבקרה תוך כדי הרצת התוכניות המודבקות.

ניתן לסכם את מאפייני הנגיפים כדלקמן:

1. הנגיפים למיניהם הם למעשה קוד תוכנה מוגדר.
2. נגיפים רבים מסתמכים על השעון הפנימי של המחשב ולכן גם מכילים פרמטרים, הקובעים את תאריך התחלת הנזק, ואת שיטת פעולת התוכנית הגורמת את הזנק. ישנם נגיפים אשר מסתמכים על מונה הסופר את מספר ההדבקות שלהם, נגיפים אחרים מחכים להופעת פקודה מסוימת כגון הפקודה COPY.
3. כל הנגיפים גורמים נזקים, אם בצורת הטרדה, האטה ושיבוש מערכת ההפעלה, תקיעת המחשב ואפילו מחיקת קבצים והרס המידע על גבי תקליטון שלם.
4. כל הנגיפים הם ברי שכפול, בשיטות שונות ומתוחכמות.

פרק 2

שיטות חלוקת נגיפי המחשב

בספרות המקצועית מוזכרים שני סוגי חלוקות של נגיפים.

חלוקה I

א. נגיף עטיפה - SHELL VIRUSES

נגיף עטיפה עוטף עצמו סביב התוכנה המארחת מבלי לשנות אותה. תוכניות עטיפה כאלו קל לכתוב, ולכן מעריכים שרוב הנגיפים (כ-50%) הינם מסוג זה.

נגיף עטיפה קל לנקות ולגלות. נגיפים אלה תוקפים קבצי הרצה כגון קבצים עם הסיומות: ???.COM ו-???.EXE.

דוגמא: נגיף הנצמד לקובץ COMMAND.COM.

ב. נגיף פולשני - INTRUSIVE VIRUSES

נגיף פולשני הינו "וירוס" הפולש לתוך תוכנית קיימת ומכניס קטע קוד לתוך התוכנית. נגיף כזה קשה לכתוב ועוד יותר קשה להוציאו מבלי לפגוע בתוכנית עצמה. "וירוס" זה תוקף בנוסף לקבצים בעלי סיומת: ???.EXE ו-???.COM גם קבצי נתונים ב-ASCII.

ג. נגיף מערכת ההפעלה - OPERATING SYSTEM VIRUSES

נגיף מערכת ההפעלה מחליף חלקים מנתוני מערכת ההפעלה בלוגיקה משלהם. הוא קשה מאד לכתיבה, ויש לו את היכולת לרכוש שליטה על המערכת בזמן האיתחול (BOOT). נגיף זה משתמש בסימון מזוייף של מקטעים (SECTOR) פגומים כדי להחביא כמות קוד גדולה. על מנת להפטר מנגיף זה צריך לבצע ארגון ברמה נמוכה (LOW LEVEL FORMAT) או כתיבה על המיקום של כל סיבית וסיבית.

ד. נגיפי קובץ מקור - SOURCE CODE VIRUSES

נגיף זה גורם להתקנת תוכנות קבועות בזכרון הגישה האקראית ([illegible]) ברכיבי המידחף (DRIVER) על מנת להדביק יעדים אחרים בזכרון.

נגיף זה יכול להשאר קבוע (TERMINATE & STAY RESIDENT - TSR) או יכול להיות מוסתר במקום כלשהו ב-RAM.

חלוקה II

א. נגיפים מדביקי התיחול - BOOT INFECTOR VIRUSES

נגיף זה מדביק עצמו לקטע המבצע תיחול (BOOT) בתקליטון או בתקליט הקשיח (HARD DISK) ונכנס לפעולה עם הדלקת המחשב, עוקב אחר כל פעולות המערכת ובודק באם הוכנס תקליטון חדש למערכת כדי להדביקו. כאשר תקליטון כזה מוכנס, מעתיק הנגיף את עצמו למקטע התיחול (SECTOR האפס) ואז הוא ממשיך ומדביק את המערכת הבאה מהתקליטון המודבק. ביצוע התיחול (BOOT) מתקליטון, זה הינו אחת הדרכים בה ניתן להדביק מערכת אחרת.

ב. נגיפים מדביקי מערכת - SYSTEM INFECTOR VIRUSES

נגיף זה מצמיד עצמו למערכת ההפעלה או ליחידות המידחף של המערכת (SYSTEM DEVICE DRIVER). נגיף זה יכול להדביק גם את מפענח הפקודות (COMMAND INTERPRETERS), ושגרת המערכת (SYSTEM) של הקלט פלט או יחידות מידחף יחודיות. הוא משתלט, עם ביצוע התיחול במערכת, ונשאר פעיל בכל הזמנים. עם הכנסת תקליטון מערכת (SYSTEM) לאחד הכוננים, הנגיף משכפל את עצמו לתוך קבצי המערכת שבתקליטון.

ג. נגיפי אב מדביקי תוכנות שימושיות GENERIC APPLICATION INFECTOR VIRUSES

נגיף זה מסוגל להדביק כל תוכנה שימושית. הוא משתלט כאשר תוכנית נגועה מורצת, הוא סורק את המערכת ובודק באם יש על התקליט הקשיח מקטעים (SECTOR) שניתן להדביקם. כאשר מוצאים "פונדקאים" חדשים נדבקים אליהם. לאחר תום הסריקה הוא מעביר את השליטה לתוכנית שבשימוש. נגיפים אלו הם הנפוצים ביותר.

חלוקה נוספת

על אף המוזכר בספרות המקצועית, ניתן לחלק את הנגיפים לשתי תת-קבוצות עקריות.

א. נגיפים המדביקים את מקטע התיחול (BOOT SECTOR).
לדוגמא: נגיף השגיאות ERROR VIRUS והנגיף הפקיסטני BRAIN VIRUS.

ב. נגיפים המדביקים את קבצי EXE. ו-COM. נגיפים אלו נצמדים למקום כלשהוא בקובץ.
לדוגמא: הנגיף הישראלי ISRAELI VIRUS ונגיף אלבמה ALABAMA VIRUS.

פ ר ק 3

מאפייני התופעה

במחשב הנגוע בנגיפים ניתן למצוא אחת או יותר מהתופעות המפורטות להלן:

1. גידול בלתי צפוי במספר הבתים בתוכנה המורצת. (ירושלמי, אלבמה)
2. תאריך הקובץ ישתנה עם הפעלת הפקודה DIR.
3. הגישה לתקליט הקשיח מבוצעת תוך נטיה גדולה יותר לשגיאות (ERROR PRONE ACCESS).
4. מספר שהמיקטעים (SECTOR) השגויים (BAD SECTOR) גדל בבת אחת. (פאקיסטני).
5. כלל פעולות המחשב ומימוש פקודות ה-DOS נעשות איטיות יותר.
6. כמות הזכרון האקראי (RAM) הפנוי קטן מהרגיל.
7. תוכניות תושב בזכרון האקראי (RAM RESIDENT PROGRAM) כגון מילון אלקלעי, תוכנית SIDEKICK ועוד עלולות לא לרוץ בצורה תקינה.
8. המחשב עשוי לא להגיב (לא בכל המקרים) להקלדת נתונים בצורה עקבית.
9. העלאת תוכנת הגיבוי על מנת לפתור בעיה כלשהיא בתוכנה נתונה עשויה לחת את אותה תסמונת ממנה בקשנו להמנע.
10. קבצים וחוצצים (DIRECTORY) עשויים להעלם בפתאומיות. (נגיף ירושלמי ופאקיסטני).
11. מתבצעת גישה לכתובת על התקליט הקשיח ועל התקליטון גם כשלא ניתנה הוראה לכך. (ירושלמי ואלבמה).
12. הריסת טבלת הקצאת קבצים (FILE ALLOCATION TABLE - FAT) דבר הגורם לאיבוד תוכנת התקליטון. (פאקיסטני).
13. שינוי השמת התקליטון (DISK ASSIGNMENTS) כך שהמידע נכתב בצורה שגויה.
14. שכפול מיותר של קבצים כדי למלא את המקום הריק בתקליטון.
15. מערכת ההפעלה מושעת (SUSPENDED) תוך כדי הרצה כך שהכניסה דרך המקשים בלתי אפשרית.
16. תוספת של קבצים נסתרים (HIDDEN FILE).

פרק 4
נוהל לטיפול ומניעת נגיפים

הכרה בבעיה הנגיפית, תביא להגברת המודעות ולנקיטת אמצעים יעילים למניעת התפשטותם. חוברת זו מפורסמת עמ"נ ל"הרחיב את האופקים" ולהציע נהלים ושיטות התמודדות עם הבעיה הנגיפית.

1. הנחה את כל המשתמשים לפעול עפ"י נוהל הכנסת תוכנה חדשה לשימוש, שמשמעה בדיקה מתאם מוסמך (אדם שמונה לכך) ובמחשב מרכזי אחד ויחיד לפני שתופץ.
2. אין להרשות קבלת תוכנות דרך רשתות תקשורת.
3. אין להשתמש בתוכנה חופשית לכל (PUBLIC DOMAIN SOFTWARE).
4. אין להשתמש בתוכנות גנובות ופירטיות (תוכנות גונבה).
5. יש למנוע לחלוטין שימוש במחשבי היחידות למשחקים העוברים בצורה חופשית בין משתמשי המחשב.
6. דאג להגן על כל תקליטון מקורי או תקליטון המכיל את ה-DOS באמצאות מדבקת הגנה (WRITE PROTECT) וכן על כל התקליטונים בהם הינך מעביר תוכנה.
7. מנע נגישות למחשבים או לתוכנות מאנשים בלתי מוסמכים.
8. המנע מהשארת תקליטונים בצורה חופשית. נעל את התקליטונים במקום בטוח.
9. הפוך את כל קבצי ה-COM וה-EXE לקבצים הנתנים לקריאה בלבד (READ ONLY FILES). אם ברשותך גירסת DOS 3.3, ניתן לעשות זאת בשני צעדים בלבד תוך שימוש בפקודה ATTRIB.

   ATTRIB + R *.COM/S

   ATTRIB + R *.EXE/S

   אם ברשותך DOS מגירסאות ישנות יותר, תאלץ לעבור בכל מחיצה בנפרד (מחיצה = DIRECTORY), ולבצע את הפקודה (6).
10. הגבל גישה לקבצים באמצאות קידוד ובקרת מסלול שיאפשרו עקיבה ותיעוד (LOGGING) אחר נגיפים חודרים (1).
11. הגבל את תחלופת התקליטונים המכילים תוכנות מסוג COM. ו-EXE..
12. באמצאות פקודת CHKDSK עקוב אחר שינויים במכלול התקליטון, בצע רישום, והשווה לרישום קודם, שינוי בלתי סביר בנתונים צריך להדליק "אור אדום", בדוק תקליטון זה.
13. אין לבצע תיחול (BOOT) למחשב מתקליטון אקראי כלשהו אלא אך ורק מתקליטון מוגדר שתפקידו יהיה ביצוע התיחול (BOOT) <u>בלבד</u>. סמן וגבה אותו. תקליטון זה חייב להיות מוגן. וודא שלכל מערכת P.C. יהיה תקליטון תיחול אחד.
14. ההגנה נגד נגיפים חייבת להיות <u>חלק בלתי נפרד</u> ממערך ההגנה הכולל.

15. בצע גיבויים בצורה עקבית ומסודרת. השתמש במספר סטים של גיבוי (גם לקבצי הרצה).

16. אין לבצע תיחול מתקליטון במערכת כאשר קיים כונן קשיח, אלא אך רק בזמן "ההתאוששות".

17. רשום לכל תקליטון תווית (VOLUME LABEL) בזמן התיבנות (FORMAT). הסתכל על התווית בזמן הפקודה DIR וזהה שינוי של התווית שלא בוצע על ידך.

18. שים לב לשינויים במבנה ותפעול המערכת. האם הרצת התוכנית לוקחת יותר זמן מהרגיל? האם יש הודעות שגיאה על התקליטון? והאם הן מופיעות בקביעות?

19. אם הינך משתמש בחקאי (EMULATION) ל-3270 המחובר למחשב גדול, שמור את תוכנית החקאי בחוצץ (DIRECTORY) נפרד. מומלץ שייעוד המחשב יהיה רק לאמולציית 3270.

20. אם הינך עובד ברשת אל תשתמש במחשב המגיש (SERVER) בתור תחנת עבודה. תן רק למנהל המערכת (SYSTEM ADMINISTRATOR) לעבוד עליו.

24. הזז את הקובץ COMMAND.COM מתוך השורש (ROOT). רשום בתוך הקובץ CONFIG.SYS את השורה הנ"ל שתגדיר מיקום חדש ל-COMMAND.COM.
SHELL = C:\HIDDEN \COMMAND.COM /P כאשר החוצץ HIDDEN יכול להיות כל שם.
רשום גם את הפקודה הבאה:
SET COMSPEC = C:\HIDDEN\COMMAND.COM
ניתן גם להחביא (HIDDEN FILE) את הקובץ ע"י הפקודה ATTRIB של ה-DOS.

25. קיימות תוכנות המציגות את התוכנות הקבועות בזכרון (RESIDENT) המחשב. השתמש בתוכנת RAMCHK או MAPMEN וגלה המצאות תוכנה לא ידועה בזכרון המחשב (RAM)

26. להדפיס חוצץ (DIRECTORY) של הקבצים ולהשוות (באמצאות ההדפסות הקודמות) את גודל קבצי תוכנות המקור (לא נתונים) וקבצי גיבוי הנתונים של התקליטונים מול גודל הקבצים המקבילים בדיסק הקשיח. אם קבצי.COM. בדיסק גדולים יותר מקבצי הגיבוי המקבילים להם, בגבולות של 1.4K - 2K בתים אזי קיים חשש שהתופעה נגרמה ע"י נגיפים. קבצי EXE. נגועים עלולים להיות גדולים הרבה יותר.

27. במקרה שאחת המחברות המחשב, או כל גוף אחר, מעוניין להדגים תוכנה חדשה, יש לבצע הדגמה זו על מחשב השייך לגוף זה.

28. אם מתקבלת תוכנה לתקופת נסיון, יש להריץ אותה על מחשב אחד בלבד, שגובה לפני תחילת השימוש בתוכנה, שיעודו יהיה לניסוי תוכנות ושחשיבותו המבצעית נמוכה.

פרק 5

מה מסוגל הנגיף לבצע

נגיף יכול להיות הרסני או לא הרסני. נגיפים שאינם הרסניים הם בדרך כלל נגיפים המטרידים את המשתמש בהודעות לא תכליתיות ומפריעים לעבודה התקינה. נגיפים הרסניים יכולים למחוק נתונים ולפגוע בחומרה.

* נגיפים מטרידים מסוגלים למשוך את תשומת לב העובד להודעה טיפשית כלשהי או לציור. כדוגמא נותנות הודעות פוליטיות או הודעות סרק. יתכן שהם ישנו את צבעי המסך, יעכבו ביצוע פקודות, יריצו כדור פינג פונג על המסך ועוד.

* נגיפים הגורמים להרס מסיבי, מבצעים זאת ע"י ביצוע תיבנות ברמה נמוכה (LOW LEVEL FORMAT) של התקליטון. במקרה זה הנתונים יהיו בלתי אפשריים לשחזור.

* השמדה חלקית היא מחיקה או שינוי של חלק ממידע על התקליטון. השמדה ברירותית (סלקטיבית) היא השמדה או שינוי של קבצים מוגדרים או קבוצות של קבצים מוגדרים.

* נגיפים הגורמים לתוהו ובוהו (HAVOC) אקראי הם המסוכנים ביותר מאחר וקשה להבחין באופיון מוגדר שבאמצעותו ניתן לאתר ולתקן את מה שביצע הנגיף. הנגיפים האלה עובדים ע"י שינוי אקראי של בית (BYTE) על התקליטון או על הזכרון האקראי (RAM) תוך כדי השימוש בתוכנה. מידע (DATA) מהכניסות או היציאות של יחידות (INPUT/OUTPUT DEVICE) משוחלף בצורה אקראית. התוצאה - זמן רב מבוזבז לגילוי מקור הבעיה, לתיקון ושיקום ההריסות. לנגיפים האלה יש תכונה לצוף ולהופיע מחדש לאחר שכביכול חוסלו.

* נגיפים הפוגעים בחומרה (HARDWARE). נגיפים אלו עלולים לפגוע במשגוח (MONITOR) וכך לגרום למחשב שלא להכיר את הכונן הקשיח (HARD DISK).

פרק 6
כיצד מתפשטים הנגיפים

* נגיפים משוגרים דרך רשתות התקשורת השונות, כגון רשת ה - BBS וכן דרך תקשורת ישירה בין מחשבים. כמו כן הם מועברים באמצאות תקליטונים מודבקים.

* נגיפים אינם יכולים לעבור בלי עזרת האדם. המחשב האישי לא ידבק אלא אם כן מישהו יריץ תוכנית הנגועה בנגיפים שונים. ברשתות מחשבים גדולות הנגיף מתפשט דרך הרשת ואומר למערכת האחרת להריץ את קוד הנגיף כמו התוכנית.

* הנגיף מתפשט גם ע"י שינויים המבוצעים במערכת. כאשר הנגיף מדביק את קבצי COM. ו- EXE., לכן כאשר תוכנה מודבקת, מורצת באחד משלבי הריצה, משתלט הנגיף ומדביק את שאר חלקי המערכת, בין אם ע"י השארות בזכרון או הדבקה בזמן הריצה. אחרי שהנגיף חודר למערכת ומשכפל את עצמו, הוא מתפשט למחשבים אחרים.

* נגיף המתפשט דרך רשת תקשורת (LAN) של מחשב אישי.

פרק 7

נגיפים על מערכת הפעלה MS-DOS

נגיף המוח הפקיסטני - PAKISTANI BRAIN

מקור: להור פקיסטון נכתב ע"י שני אחים בתור ניסוי כדי למנוע מאנשים להעתיק תוכנה.

תאריך: ינואר 86.

יעד: מחשבי IBM PC ותואמים.

סוג: מזהם מיקטע תוך כדי תיחול - BOOT SECTOR INFECTOR.

תיאור: מחליף את מיקטע התיחול (BOOT SECTOR) המקורי ומזיז אותו למקום אחר. מוסיף 7 מיקטעים המכילים את הנגיף ומסמן את המיקטעים ששינה בתור מיקטעים שאסור להשתמש בהם כדי להגן על עצמו. מכפיל את עצמו לכל דיסקט שניתן לעשות ממנו תיחול.

התפשטות: ביצוע התיחול מתוך תקליטון נגוע. ההדבקה נעשית ע"י ביצוע פעולה כל שהיא בתקליטון הלא נגוע כגון, ראיית DIRECTORY, והרצת תוכנית . במידה והמחשב מחובר ברשת, דרך הרשת.

סימנים: יש סימון (LABEL) מיוחד "COPYRIGHT @BRAIN" המופיע עם הרצת התקליטון או הכונן הקשיח המודבק. תהליך התיחול איטי במקצת. מבצע גישות רבות לדיסק תוך הרצת תוכנות פשוטות. תוכנות יוצאות ל-DOS בפתאומיות. משנה את וקטור הפסיקות (INTERUPT VECTOR).

נזק: יכול לגרום לאיבוד נתונים. מתפשט מהר בתקליטונים ברי תיחול (BOOTABLE).

מניעה: אל תבצע תיחול מתוך תקליטון לא מוכר. עשה תיחול רק מתוך כונן קשיח (HARD DISK) באם קיים, ואם לא מתוך תקליטון המיועד לביצוע תיחול ומוגן ע"י מדבקה.

שחזור: כבה את המחשב ובצע תיחול מתוך תקליטון נקי שמוגן עם מדבקה.חפש תקליטונים עם התווית "@BRAIN". אם מצאת, מחק את הדיסקט בעזרת הפקודה "FORMAT" או בצע העברת SYSTEM בעזרת הפקודה "SYS" ולאחר מכן שנה את התווית בעזרת תוכנית מתאימה.

הערות: א. הנגיף הנ"ל ימשיך להתקיים אחרי התיחול. יצאו מספר גרסאות וכרגע קיימת גירסה V.9.

ב. למספר גירסאות יש תווית (LABEL) שונה כדוגמא: BUFUED או ASHAR.

ג. בדיקת מקטע התיחול תגלה על תקליטון ותקליט קשיח נגוע את ההודעה הבאה (ההודעה עדכנית לגירסא V.1).

```
WELCOME TO THE DUNGEON
@ 1986 BASIST & AMAJAD (PUT) LTD &
BRAIN COMPUTER SERVICES
730 NIZAM BLOCK ALLAMA IGBAL TOWN
LEHORE, PAKISTAN
PHONE : 430791, 443248, 2800530
BEWARE OF THIS VIRUS
CONTACT US FOR VACCINATION
```

נגיף "כחול לבן" או הנגיף הירושלמי - ISRAELI VIRUS

מקור: האוניברסיטה העברית בירושלים.

תאריך: דצמבר 87.

יעד: מחשבי IBM ותואמים.

סוג: נגיף אב המדביק תוכנה שימושית GENERIC APPLICATION INFECTOR.

תיאור: מדביק את כל קבצי ה- COM. ו-EXE. ומגדיל את התוכניות. תוכנות מודבקות משתנות, והופכות לתוכנות שנשארות בזכרון (AND STAY RESIDENT - TSR TERMINATE). התוכנות נדבקות בנגיף כאשר הן מורצות בתוך מערכת נגועה. גם תקליטונים וגם כוננים קשיחים יכולים להידבק.

התפשטות: מועבר ממקום למקום ע"י תקליטונים נגועים.

סימנים: מאיט את המערכת. תוכניות EXE. גדלות עד שכבר אי אפשר להריץ אותן. הזכרון הפנוי קטן.

נזק: סוגים מסוימים מוחקים את כל הנתונים על הכונן הקשיח. יתכן ותוכניות יעלמו פתאום. תוכניות נעלמות בכל תאריך שהוא שילוב של יום שישי ה-13 לחודש (באם יש שעון במחשב). יצויין כי באוקטובר הקרוב (1989) יום שישי יחול בתאריך 13 לחודש.

מניעה: אין להריץ תוכניות מתוך מקורות לא ידועים. אין לאחסן תקליטונים המכילים תוכניות שניתן להריץ עם הנתונים. בדוק את גודל הקבצים ועקוב אחר שינויים.

שחזור: כבה את המחשב ובצע תיחול מתקליטון מוגן עם מדבקה. מחק את כל הקבצים עם הסיומת .COM .EXE על התקליט הקשיח ועל התקליטונים. החלף את התוכניות בעזרת התקליטונים המקוריים.

הערות: לנגיף זה יש מחרוזת זיהוי והיא "SUMSDOS". בגרסאות מתקדמות של הנגיף הוחלפה מחרוזת הזיהוי במחרוזות אחרות כגון "URI2V21" (13).

נגיף מסוג - ALAMEDA VIRUS

מקור: אוקלנד, קליפורניה.
תאריך: אביב 88.
יעד: מחשבי IBM PC ותואמיו.
סוג: מזהמי תיחול - BOOT INFECTOR.
תיאור: מחליף את מקטע התיחול (BOOT SECTOR) עם עצמו ומאחסן את מקטע התיחול המקורי במקטע פנוי. מדביק באמצאות תיחול חוזר (REBOOT). לא מסמן את מקטע התיחול המקורי בתור לא שמיש(UNSAUBLE SECTOR).
התפשטות: ביצוע תיחול מתקליטון מזוהם. לאחר מכן הכנסת תקליטון מערכת (SYSTEM) נקי לתוך מערכת נגועה. דרך רשתות תקשורת במידה והמחשב מחובר ברשת.
סימנים: האטת קצב התיחול. נפילות מערכת, איבוד נתונים.
נזק: איבוד נתונים.
מניעה: בצע תיחול אך ורק מתוך תקליטון עם מדבקת הגנה. אל תבצע תיחול לכונן קשיח (HARD DISK) מתוך תקליטון. אל תעביר תקליטון מערכת (SYSTEM) ממחשב למחשב.
שיחזור: כבה את המחשב. בצע תיחול מתוך תקליטון מקורי עם הגנה נגד כתיבה (מדבקת WRITE PROTECT) בצע את הפקודה .SYS כדי להחליף את מקטע התיחול (BOOT SECTOR).
הערות: אינו מגן על מקטע התיחול המקורי כמו הנגיף הפקיסטני, ולכן יתכן שיכתב על המקטע המכיל את המערכת (SYSTEM) במקרה כזה תהיה הודעה של "BOOT FAILURE".

נגיף מסוג - LEHIGH VIRUS

מקור: אוניברסיטת LEHIGH.

תאריך: סוף שנת 87.

יעד: מחשבי IBM PC ותואמים.

סוג: מדביקי התיחול - BOOT INFECTOR.

תיאור: מדביק את ה COMMAND.COM, משנה את גודלו בערך ב- 20 בתים, משנה את תאריך וזמן יצירתו של הקובץ.

התפשטות: שימוש בתקליטונים מזוהמים או הכנסת תקליטון נקי לתוך מערכת נגועה. דרך רשתות תקשורת במידה והמחשב מחובר ברשת.

סימנים: שינויים בגודל קובץ ה COMMAND.COM. איבוד כל נתוני המערכת.

נזק: הריסת כל הנתונים. מופעל לאחר ארבע פעמים של הדבקה ואז הורס את כל נתוני המערכת, בין אם מדובר בתקליטונים ובין אם מדובר בתקליט קשיח.

מניעה: אל תשתמש בתקליטון המערכת להעברת תוכנות אחרות. אל תכניס תקליטון מערכת לתוך מחשב אחר. שים לב לזמן ולתאריך וכן לגודל קובץ COMMAND.COM.

להלן גדלים של הקובץ COMMAND.COM:

17792 בתים	DOS 2.1
23791 בתים	DOS 3.2
25307 בתים	DOS 3.3
37637 בתים	DOS 4.0

שחזור: כבה את המחשב. בצע תיחול (BOOT) מתקליטון מקורי ומוגן. בטל את הקובץ COMMAND.COM מתוך התקליט הקשיח וכן מתוך כל התקליטונים הנגועים. העתק את קובץ COMMAND.COM מתקליטון מקורי, ובצע את פקודה ה-SYS. העתק את הקובץ COMMAND.COM מתקליטון מקורי.

הערה: לנגיף זה תקופת דגירה קצרה מאד (רק ארבע הדבקות) ולכן חשוב מאד לגלותו בטרם יגרום נזקים.

נגיף מסוג פינג פונג - PING PONG VIRUS (או ITALIAN VIRUS)

מקור: לא ידוע.

תאריך: אמצע שנת 88.

יעד: מחשבי IBM PC ותואמים.

סוג: מדביקי התיחול BOOT INFECTOR.

תיאור: מדביק את מקטע התיחול (BOOT SECTOR). הנגיף משוכפל אל תוך מקטע התיחול (BOOT SECTOR) של התקליט הקשיח או של התקליטון. הנגיף הנמצא במחשב אינו נוגע לרעה בקבצים. בפרקי זמן משתנים מועבר הנגיף אל הזכרון הפנימי של המחשב ומתיישב שם כתוכנה קבועה (RESIDENT), אז הוא גורם לכדור המרצד על המסך בדומה לכדור פינג-פונג.

התפשטות: ביצוע תיחול מתוך תקליטון נגוע והכנסת תקליטון נקי למערכת נגועה.

סימנים: הופעת כדור פינג-פונג.

נזק: נזק לכוננני המחשב עקב הפעלתם בצורה קיצונית הגורמת לשחיקתם המואצת.

מניעה: בצע תיחול אך ורק מתוך תקליטון עם מדבקת הגנה. אל תבצע תיחול לכונן קשיח (HARD DISK) מתוך תקליטון. אל תעביר תקליטון מערכת (SYSTEM) ממחשב למחשב.

שחזור: ביצוע הפקודה SYS. לתקליטון/כונן קשיח. העתק את הקובץ COMMAND.COM מתקליטון מקורי.

הערות: א. לא ניתן להשתחרר מהנגיף ע"י כיבוי המחשב, כי תקליטוני התיחול נגועים, ויש לטפל בהם.

ב. הפקודה SYS. חייבת להיות באותה גירסה של ה-DOS הקיים במערכת.

ג. כנראה קיימות שלוש גירסאות של נגיף זה. שתי גרסאות ראשונות כנראה פוגעות בכוננני הדיסקטים ואלו גירסה שלישית מוחקת את ה-FAT (FILE ALLOCATION TABLE).

נגיפי רשתות - FLU-SHOT 4 VIRUSES

מקור: רשתות תקשורת (BBS).

תאריך: מרץ 88.

יעד: מחשבי IBM PC ותואמים.

סוג: לא ידוע.

תיאור: המשתמשים חשבו שנגיף זה הינו גירסה חדשה לתוכנה אנטי-נגיפית - FLU-SHOT 3, הזיהויים והמלל שנראה על המסך היו זהים לתוכנה המקורית. אחרי מעבר של מספר מסכים בהם מוסברת מטרת התוכנית, המשתמש נותן את המבנה בו הוא רוצה שהתוכנה תותקן על המחשב. די בקריאת המלל בשביל להפעיל את הנגיף.

התפשטות: העתקה מרשתות תקשורת או העתקה של קבצים נגועים.

סימנים: לא ידוע.

נזק: הנגיף מוחק קטעים (CLUSTERS) מהדיסק ומזהם את מקטע אפס.

מניעה: אין להוריד נתונים מרשתות תקשורת.

שחזור: לא ידוע.

הערות: אין.

נגיף המסך (נגיף השגיאה) - ERROR VIRUS

מקור: לא ידוע.

תאריך: לא ידוע.

יעד: מחשבי IBM PC ותואמים.

סוג: מדביקי התיחול - BOOT INFECTOR.

תיאור: לנגיף זה מספר גרסאות, אחת מהן מחליפה אותיות על המסך ולדוגמה: מחליפה אות א' באות ע' ולהיפך, אות כ' באות ח' וכו'. גרסאות שונות יכולות להחליף מספרים על המסך. כשהוא מופעל הוא הופך לתוכנה הנשארת בזכרון (TSR- TERMINATE & STAY RESIDENT).

התפשטות: ביצוע תיחול מתוך תקליטון נגוע והכנסת תקליטון נקי למערכת נגועה.

סימנים: טעויות רבות ברישום על הצג (MONITOR).

נזק: אי דיוק בנתונים.

מניעה: אל תשתמש בתקליטון המערכת להעברת תוכנות אחרות. אל תכניס תקליטון המערכת לתוך מחשב אחר.

שחזור: ביצוע הפקודה SYS. לתקליטון/תקליט קשיח והעתקת הקובץ COMMAND.COM.

הערות: באחת הגרסאות של הנגיף הוא נקרא נגיף שגיאות נוח. נגיף זה הינו גירסה של נגיף הפינג-פונג, שגרת ציור הכדור הוחלפה בשגרה המחליפה אותיות. לכן הטיפול בו, כמו הטיפול בנגיף הפינג-פונג.

נגיף DBASE - DBASE VIRUS

מקור: לא ידוע.

תאריך: לא ידוע.

יעד: מחשבי IBM PC ותואמים, תוכנת DBASE.

סוג: לא ידוע.

תיאור: נגיף זה הינו תוכנה הנשארת בזכרון(TSR - TERMINATE AND STAY RESIDENT) העובדת בצורה דומה לנגיף הירושלמי. הנגיף עוקב אחר כל קבצי ה-DBASE (סיומת DBF.) עליהם עובדים וכעבור 90 יום הוא מוחק את טבלת הקצאות הקבצים(FAT-FILE ALLOCATION TABLE). כאשר הנגיף מופעל, הוא גורם לכך שנתונים בתוך קבצי ה-DBASE יהיו חסרי משמעות. נגיף זה יוצר קובץ נסתר בשם BUG.DAT כדי לעקוב אחר קבצי ה-DBASE.

התפשטות: לא ידוע.

סימנים: לא ידוע.

נזק: הריסת המידע על התקליטון.

מניעה: צירת קובץ קריאה בלבד (READ ONLY) בשם BUG.DAT.

שחזור: לא ידוע.

הערות: אין.

נגיף אלבמה (נגיף צרפתי) - ALABAMA VIRUS

מקור: אלבמה ארה"ב.

תאריך: הגיע לארץ בתחילת 89.

יעד: מחשבי IBM PC ותואמים.

סוג: נגיף אב מדביק תוכנה שימושית GENERIC APPLICATION INFECTOR

תיאור: הנגיף נכתב באלבמה ארה"ב במסגרת המלחמה במעתיקי תוכנה. הנגיף מדביק רק קבצי EXE. כל קובץ מוגדל ב-1540 בתים (נדבק בסוף הקובץ). הנגיף מסוגל להדביק ספריות שלמות (DIRECTORIES) בבת אחת. לנגיף מונה, כאשר המונה מגיע ל-9 מופיעה הודעה והמחשב נתקע.

התפשטות: פעולת ההדבקה של המחשב נגרמת רק כאשר מורצת תוכנית מודבקת מכונן תקליטונים או תוכנית מודבקת שהועתקה אל הכונן הקשיח.

סימנים: הגדלת קבצי ה-EXE. ב-1540 בתים.

נזק: המחשב נתקע ועל המסך מוצגת, בתוך מסגרת מהבהבת, ההודעה הבאה.

```
Software Copies are prohibited by international law
BOX 1055 TUSCAMBIA ALBAMA USA
```

מניעה: השתמש רק בתוכנות מקוריות.

שחזור: העלה מגיבוי את התוכנות הנגועות.

הערות: אין.

נגיף האחד באפריל - 1ST OF APRIL VIRUS

מקור: לא ידוע.

תאריך: לא ידוע.

יעד: מחשבי IBM PC ותואמים.

סוג: מדביקי התיחול BOOT INFECTOR.

תיאור: זהו נגיף הגורם לתקיעת המחשב הנגוע בסיום תהליך התיחול שיבוצע בראשון לאפריל בלבד.

התפשטות: ביצוע תיחול מתקליטון נגוע.

סימנים: בתאריך ראשון לאפריל לאחר התיחול המחשב נתקע.

נזק: בתאריך ראשון לאפריל המחשב יתקע בסיום תהליך התיחול ויתן את ההודעה: "April 1st HA HA HA HA HA YOU HAVE A VIRUS".

מניעה: בצע תיחול אך ורק מתוך תקליטון עם מדבקת הגנה. אל תבצע תיחול לכונן קשיח (HARD DISK) מתוך תקליטון. אל תעביר תקליטון מערכת (SYSTEM) ממחשב למחשב.

שחזור: הדרך לעקוף את הבעייה הינה להעלות את המחשב מכונן :A עם מערכת ההפעלה, מתקליטון חיצוני שאינו נגוע ולתת למחשב תאריך אחר.

הערות: אין.

נגיפים הפעילים על מחשבי מקינטוש

נגיף מסוג - MACMAG

מקור: ריצ'רד ברנדו עורך מגזין MacMag, ותוכניתן דרו דוידסון מאריזונה.

תאריך: דצמבר 87.

יעד: מחשבי מקינטוש.

סוג: מזהם מקטע תוך כדי תיחול - BOOT SECTOR INFECTOR.

תיאור: נגיף Macmag חודר למערכת ע"י תוכנה נגועה ומתקין עצמו בקובץ איתחול המערכת כ - INIT. במקור הנגיף לא נועד להתגלות לפני 2 מארס 88, מועד בו הייתה צריכה להופיע הודעה על המסך והנגיף היה אמור להשמיד את עצמו. אם המחשב (מקינטוש) לא הופעל ב-2 במארס, לא ניתן היה לראות את ההודעה, מפני שהנגיף היה אמור להשמיד עצמו במועד זה, אולם התברר שגרסאות שונות של הנגיף עדיין פוגעות במשתמשי מקינטוש, אם כי במספרים קטנים.

התפשטות: הרצת תוכנה נגועה.

סימנים: האטת פעולת המערכת, בתיק קבצי המערכת קיים תיק (קובץ) בשם INIT. בתאריך 2 מארס נותן הודעה.

נזק: האטת פעולת המערכת.

מניעה: ביטול קובץ INIT מתוך המערכת וכל הקבצים הנגועים בנגיף.

שחזור: לא ידוע.

הערות: הנגיף יכול להדבק גם לתוכנה הנקראת FreeHand.

נגיף הניקוד - VIRUS SCORES

מקור: חברת SYSTEM DATA ELECTRONIC.

תאריך: סוף שנת 1987.

יעד: מחשבי מקינטוש.

סוג: נגיף אב המדביק תוכנה שימושית INFECTOR APPLICATION GENERIC.

תיאור: מדביק את כל התוכנית. מגדיל את גודל התוכנית בערך ב-7000 בתים. מחפש אפשרות התפשטות בהפסקות של 3.5 דקות. מחפש שמות של קבצים מסויימים כדי להרוס ולמחוק אותם. יוצר קבצי NOTEPAD וכן וקבצי ארכיון (SCRAPBOOK) בתוך ה-FOLDER. יוצר קבצי INVISIBLE SCORES AND DESKTOP.

התפשטות: ע"י החלפת תקליטונים נגועים או הכנסת תקליטון נגוע למערכת.

סימנים: נפילות מערכת, הקבצים גדלים. קשיים בהרצת תוכנית ה-MAKEDRAW, בהדפסה מתוכנות שונות, ובשימוש באפשרות "קבע תוכנה "מובילה" (SET START UP). קושי בהרצת גיליון אלקטרוני (EXEL). כדי לבדוק אם המחשב מזוהם יש לפתוח את תיק המערכת (SYSTEM FOLDER) ולבדוק אם קובץ הארכיון (SCRAPBOOK) או ה- NOTEPAD נראה כמו צלם (ICON) של מקינטוש או כצלם של מסמך רגיל (צילום דף עם אוזן ימין מקופלת) הראשון אמור להיות הצלם הנכון.

נזק: איבוד נתונים כתוצאה מנפילות מערכת.

מניעה: אין להחליף תקליטונים עם אנשים אחרים ואין להכניס תקליטונים עם תוכנות לתוך מחשבים של אנשים אחרים. אל תריץ תוכנות שהמקור שלהן איננו ידוע.

שחזור: בצע גיבוי <u>לכל קבצי הנתונים</u>, לא לתוכנות הניתנות להרצה. מחק את תקליט הקשיח הנגוע, ואת התקליטונים הנגועים. שחזר את קבצי המערכת והתוכניות מתוך התקליטונים המקוריים. שחזר את קבצי הנתונים.

הערות: אין.

נגיף מסוג - nVIR

מקור: המבורג גרמניה.

תאריך: קיץ 87.

יעד: מחשבי מקינטוש.

סוג: נגיפי אב מדביקי תוכנה GENERIC APPLICATION INFECTORS.

תאור: נגיף ה-nVIR מופיע בהרבה צורות, וכל צורה עם מאפייניה. המפיץ של הנגיף אחראי על הגרסאות השונות אבל צורת ההדבקה דומה מאד. שמים את ה-nVIR בתוך קבצי המערכת, ובמקרה ותוכנית השרות נדבקה, כל תוכניות השרות האחרות ידבקו.

התפשטות: הכנסת תקליטון נגוע למערכת והפעלת התוכנית הנגועה. דרך רשתות תקשורת במידה והמחשב מחובר ברשת.

סימנים: יש הרבה סימנים, כתוצאה מהגרסאות הרבות. דוגמאות לסימנים: נפילות מערכת, צפצופים עם קול האומר "DON'T PANIC". קבצים נעלמים, וכו'.

נזק: איבוד נתונים. נפילות מערכת תכופות.

מניעה: יש לעבוד עם תקליטונים מקוריים בלבד.

שחזור: בצע גיבוי לקבצי נתונים. מחק תקליטונים נגועים, שחזר תוכניות מהמקור ושחזר את קבצי הנתונים.

הערות: הרסני במיוחד ויכול להדביק מערכות תוך מספר מועט של דקות. מתלבש על תיק המערכת (קובץ בלתי נראה).

פרק 8

תוכנות נגד נגיפיות הקיימות למערכות הפעלה MS-DOS

בפרק זה ניתנת סקירה קצרה על התוכנות הקיימות נגד נגיפים, התוכנות מוצגות ברמה כללית, אך יעילותן לא נבדקה, וזאת על מנת להשלים תמונה מאוזנת.

תוכנות שמקורן בחו"ל:

.1 C-4 מהדורה 1.22

מקור: InterPath

דרישות: 12K RAM, כל סוגי ה-DOS, רצוי כונן קשיח.

תיאור: מסוגל לגלות ולמנוע חלק מזיהומי הנגיפים. C-4 נכנס לזכרון כ-TSR וכמו כל תוכנית איתור הנגיפים האחרות ה C-4 ידווח מדי פעם אזעקות שווא. ישנן מספר פקודות DOS כגון FORMAT, FDISK או תוכנות אחרות כמו NORTON המסוגלות לדרבן (TRIGGER) הופעת אזעקות השוא. התוכנה פועלת על התיחול מגינה על פסיקות (INERRUPT) ה-DOS, על מקטע התיחול, על הקובץ COMMAND.COM, קבצי ה-FAT, קבצים חסויים וכו'. התוכנה חופשית להעתקה.

.2 CERTUS (ידועה גם כ-CORPORATE VACCINE) מהדורה 2.1

מקור: FOUNDATION WARE.

דרישות: 512K RAM, 3.0 DOS ומעלה.

תיאור: התוכנה עושה כמעט את כל הדברים הנדרשים ונחשבת לאחת התוכנות הטובות ביותר. היא מורכבת מ-43 תוכניות ולכן היא מבצעת הרבה דברים, החל מביצוע מעקב (LOG), שיחזור FAT, וכלה בהגנה על מקומות רגישים ב-DOS. התוכנה מאפשרת גם חתימה על קבצים, ושמירת העתקים של ה-FAT, שימוש ב- CRC ובסיסמאות. גדולתה של התוכנה, היא בכושרה לאתר נגיפים ולהשמידם. אם כי היא קשה לטיפול - התוכנה חופשית להעתקה.

.3 DISK WATCHER מהדורה 2.0

מקור: RG Software System.

דרישות: 47K RAM, DOS 2.0 ומעלה.

תיאור: תוכנה "חזקה" במיוחד בתור "תוכנת ניהול קבצים" אבל לא באיתור ובהשמדת נגיפים. התוכנה עוקבת אחר כל פעילות חריגה במערכת. במקרה של שינוי בקבצי EXE. ו-COM. תופיע הודעה למשתמש. אזהרה תופיע גם במקרה שיש קבצים מוסתרים (HIDDEN FILE) חוץ מקבצי המערכת. התוכנה חופשית להעתקה.

4. DR. PANDA UTILITIES מהדורה 3.3

מקור: Panda Systems.

דרישות: 3K RAM, 2.1 DOS ומעלה.

תאור: התוכנה מחפשת פעילות חשודה בתקליטון, מקבלת בקשות לכתיבה על כתובת מוחלטת (ABSOLUTE ADDRESS) של המקטע ועוקבת אחר פעולות מסוכנות כמו FORMAT ובדיקת שלמות קבצים. התוכנית בודקת קבצים מוסתרים (HIDDEN FILES), מגינה על אזורים רגישים ב-DOS (BOOT SECTOR, PARTITION TABLE). בתוכנה קיימת תוכנית מיוחדת נגד הנגיף הפקיסטאני. החסרון הגדול של התוכנה הוא שיש להפעילה בתהליך התיחול ולא לאחר מכן. התוכנה אינה מוגנת.

5. FLU-SHOT+ מהדורה 1.5

מקור: Software Concepts Design.

דרישות: 265K RAM, 2.0 DOS ומעלה.

תיאור: זוהי תוכנה עם כושר פעולה רחב, התוכנה מסוגלת לבחור את כל סוגי ההגנות בהם המשתמש מעוניין. ברירת המחדל מגינה על כל קבצי המערכת עם CHECKSUM תתכן בעייה בעבודה עם גרפיקה. התוכנה אינה מוגנת.

6. MACE VACCINE מהדורה 1.1

מקור: Paul Mace Software.

דרישות: 256K RAM, 2.0 DOS ומעלה.

תיאור: התוכנה מגינה בשתי רמות. רמה ראשונה מגינה בפני כניסה לקבצי המערכת וברמה השניה, מפני שימוש בתוכניות שנכנסות לתקליטון ומסוגלות לפגוע בו כמו FORMAT, PCTOOLS, NORTON, DEBUG, CHKDSK/F ועוד. נגיף שתוקף את המערכת לפני הרצת MACE VACCINE אינו מתגלה. התוכנה קלה במיוחד לשימוש - ואינה מוגנת.

7. SOFTSAFE מהדורה 1.6

מקור: Software Directions INC.

דרישות: 4K RAM, 3.0 DOS ומעלה.

תיאור: שילוב של שתי תוכנות, הראשונה מגינה על קבצי המערכת, והשניה בודקת את הקבצים המורצים. התוכנה מגינה על הכונן הקשיח בסיסמא (עד 8 סיסמאות). בתור תוכנה להצפנת נתונים ושימוש בסיסמאות התוכנה מומלצת, אך בתור תוכנת נגד נגיפית התוכנה אינה מומלצת. לסיכום זוהי, בעיקרה תוכנית הצפנה, ולא תוכנה לאיתור ומיגור נגיפים, (היא אומנם מכילה תוכנית VSCHECK.EXE). התוכנה אינה מוגנת.

8. VACCINE (עבור מערכת DOS) מהדורה 2.3

מקור: WorldWide Data Corp.

דרישות: 5K RAM, DOS 2.0 ומעלה.

תיאור: אם יש נגיף במערכת בודק קבצי OVL. COM. EXE. התוכנה הנ"ל בנויה משלוש תת תוכניות.

א. תוכנית נגד נגיפית ANTIDOTE.

ב. תוכנת בדיקה CHECKUP.

ג. תוכנת "תרכיב".

כולם ביחד וכל אחד לחוד בודקים את התוכנה. מבצעת CHECKSUM עד 1300 קבצים (אפשר יותר). התוכנה אינה מוגנת.

9. VIRUSAFE מהדורה 1.6

מקור: COMNETCO INC.

דרישות: 7K RAM, DOS 2.1 ומעלה.

תיאור: התוכנה מחולקת לשלושה חלקים, שניים מהם סבילים. והם בדיקת הנגיף ובדיקת שלמות התוכנית (INTEGRITY CHECKER), התוכנית השלישית הינה תוכנית TSR. הדרך הטובה להריץ את התוכנית היא מה-AUTOEXEC. אחת מהתוכניות הסבילות בודקת המצאות נגיף בזכרון, והשניה בודקת גודל קובץ ועוד מיצדים (PARAMETER) כמו CHECKSUM. התוכנית השלישית מיועדת לגילוי ומניעת חדירת נגיף. קיימות שתי בעיות לתוכנה.

א. היא אף פעם לא מזהירה בפני נגיפים.

ב. התיעוד גרוע חסר פרטים והסברים.

התוכנה אינה מוגנת.

10. VIRUS GUARD מהדורה 1.5

מקור: IP TECHNOLOGIES.

דרישות: 128K RAM, DOS 2.1 ומעלה.

תיאור: הפילוסופיה העומדת מאחורי תוכנה זו, הינה העובדה כי קבצים אינם יכולים להזדהם לבד - מישהו צריך לזהם אותם. ולכן VIRUS GAURD מונע מתוכניות מזוהמות לרוץ. ובכך מונע מהזיהום להתפשט. התוכנה מתחלקת לשני חלקים, חלק ראשון תוכנה המבצעת חתימה (SIGNATURE) לקבצים וחלק שני הוא תוכנה לבדיקת ואימות החתימה. התוכנה הזו אינה משוכללת אבל בהחלט מבצעת את הנדרש במסגרת ההגבלות של התוכנה. התוכנה אינה מוגנת.

11. VIR-X מהדורה 1.2

מקור: MICRO CRAFT.

דרישות: 128K RAM DOS 2.1 ומעלה.

תיאור: התוכנה בנויה משלושה חלקים:

א. ה-PROTEK שהוא חוצץ מורחב.

ב. ה-DETEK המבקר את כל הפעילות הנגיפית.

ג. ה-DISKLOK שהיא תוכנת TSR.

התוכנית מאפשרת מספר רמות של הגנה, אותם יבחר המשתמש, היא יעילה במיוחד כנגד נגיפי TSR. התוכנה אינה מוגנת.

תוכנות שמקורן בארץ

תוכנות מסחריות:

VIRUS SAFE

חברה: "אלישים".

תיאור: חבילת תוכנה עם חמש פונקציות .

א. זיהוי נגיפים היושבים בתור תוכנות קבע בזכרון (RESIDENT).

ב. איתור תופעות חשודות כמו נסיון לכתוב על קבצי EXE. COM., נסיון של תוכניות בלתי מזוהות להתישב בזכרון. (קיימת טבלה עם רשימה של תוכניות המותר להן להתיישב בזכרון).

ג. זיהוי, איתור וניקוי נגיפים ממשפחת ה-BOOT SECTOR (UNPONG).

ד. זיהוי, איתור וניקוי נגיפים הנדבקים לקבצי EXE. COM (UNVIRUS).

ה. פונקציה של בדיקת שלמות (INTEGERITY CHECK). נבדק לגבי ה-DATA של מקטע התיחול (BOOT SECTOR), קבצים ועוד. פונקציה זו אמורה לתת פתרון גם לנגיפים שאינם מוכרים עדיין.

את תהליך ההדבקה ניתן לחלק לשלושה חלקים נפרדים כל חלק מכיל פונקציה אחת או יותר:

שלב ראשון: לפני ההדבקה כאן בודקים (INTEGRITY CHECK) שלמות של קבצים, CHECKSUM (בדיקה אם תוכן הקובץ השתנה) בבדיקה זו נשתמש בתוכנית PIC שתפקידה לסמן קבצים ולבדוק אם הם השתנו.

שלב שני: בזמן ההדבקה קיימות שתי תוכניות.

1. VC - VIRUS CHECK, בודקת אם קיים נגיף במחשב. התוכנה מזהירה בקולות ובצפצופי סירנה עולים ויורדים והבהוב הודעת אזהרה על המסך.

2. VS - VIRUS SAFE, תוכנית זו הינה התשובה המוּחצת להפסקת התפשטות הנגיף.

שלב שלישי: תיקון הקובץ הפגוע. קיימות שתי תוכניות:

1. UNVIRUS - מתקנת קבצי EXE. ו- COM. . דוגמא לנגיפים שתוכנה זו מתקנת הם: ירושלמי, אלבמה ועוד.

2. UNPONG - מתקנת את מיקטע התיחול (BOOT SECTOR) בו פוגעים נגיפים כגון נגיף הפינג-פונג, פאקיסטני ועוד.

הערות: התוכנה רצה עם תוכניות נוספות בזכרון ללא שום בעיות. פשוטה וקלה להפעלה. התוכנה מוגנת בפני העתקה.

אנטי וירוס

חברה: "איריס".

תיאור: אנטי וירוס מאתר את הנגיפים במחשב שלך, משמיד את הנגיפים ומשקם את התוכניות הנגועות, מחסן בפני הדבקה עתידית. התוכנה בנויה משתי תוכניות:

1. IMMUNE - חיסון: תוכנית זו הינה תוכנית הנשארת בזכרון (RESIDENT) ומונעת מנגיף להכנס ולנסות להדביק את המחשב.
2. CURE - ניקוי: מנקה את הקבצים מנגיפים שנמצאו. התוכנה יכולה לתת את שמות הקבצים שנוקו, מסך עזרה, הדפסה של האינפורמציה, סטטיסטיקות שונות ועוד.

התוכנית מכירה את כל הנגיפים הקיימים בארץ; ראשון באפריל, יום שישי ה-13, פינג-פונג, פקיסטני, שגיאות, אלבמה, מריחואנה. התוכנה בודקת את מנגנוני ההדבקה של כל אחד מהנגיפים (וכן מוטציות שלהם) ולכן נגיפים חדשים הדומים לנגיפים הקיימים יתגלו. כשיתגלה נגיף חדש תוציא החברה גירסה חדשה.

הערות: התוכנה מאד פשוטה להפעלה, קלה לשימוש. תוכנה מוגנת.

V-ANALYST

חברה: "קומסט" ("COMSET").

תיאור: בנוי על אלגוריתם מתמטי המאפשר ביצוע חתימה על קבצים. V-ANALYST בנויה כך שהיא בונה מבנה נתונים המכיל חתימה (SIGNATURES) של קבצים שניתן להריצם. לכן כל שינוי המתבצע בקבצים מתגלה כיוון שהוא גורם לחתימה להשתנות. התוכנה בודקת נגיפים כאשר היא עוקבת אחר שינויים בקבצי ההרצה. הבדיקות הללו אינן מבוצעות רק לקבצים כי אם גם לקטעים חשובים בתקליטון כגון: מיקטע התיחול (BOOT SECTOR) ועוד. המשתמש מריץ את V-ANALYST על הקבצים שהוא מעויינן וכל שינוי שיבוצע בקבצים אלו יוודע. להלן רשימת הבדיקות שהתוכנה מבצעת:

1. בזמן תהליך התיחול (BOOT) בדיקת הקוד המורץ (BOOT SECTOR, PARTITION TABLE).
2. בדיקת קבצי המערכת (IBMBIO.COM) בזמן תהליך התיחול, הבדיקה מתבצעת על ידי בדיקת החתימה.
3. בדיקה שאין שני קבצים עם שם דומה (FILENAME) וסיומת שונה (EXE, COM) הן באותו חוצץ (DIRECTORY) והן באותו PATH.

התוכנה בנויה משתי תוכניות:

1. V-UNVIRUS: מגלה נגיפים קיימים ומנקה את התוכנית.
2. V-IMMUNE: מונע התפשטות נגיף. תוכנה הנשארת בזכרון (RESIDENT).

תוכניות PUBLIC DOMAIN

ישנן הרבה תוכניות PUBLIC DOMAIN שתפקידן הוא נגד נגיפים. תוכניות אלו נותנות אשלייה של הגנה. האשליה נובעת מכך שכל הזמן צצות גרסאות חדשות של נגיפים כאשר לרוב תוכניות אלו אין עדכון גרסאות ואין ברשותם את כל סוגי הנגיפים.

התוכנה היחידה לה יוצאת מדי פעם גירסה חדשה הינה התוכנה של יובל רכבי UNVIRUS כרגע אנו עומדים על גירסה 6.0 . אך תוכנה זו אינה מחסנת בפני כל הנגיפים הקיימים בארץ.

UNVIR

מחולקת לשלוש תוכניות.

1. UNVIR - תוכנה היושבת דרך קבע בזכרון ומזהירה בפני נגיפים המנסים לחדור למערכת. במידה ותוכנה כלשהי מנסה לבצע פעולה חשודה תופיע אזהרה על מסך המחשב והמשתמש יצטרך להחליט באם ברצונו להמשיך בפעולה או להפסיקה.
2. BUNVIR - מנקה את נגיף הפינג-פונג והפקיסטני.
3. ANTVIR - מנקה תוכניות מנגיף הראשון באפריל.

הערות: התוכנה אינה מזהה את כל הנגיפים הקיימים בארץ (אלבמה, שגיאות ועוד). יצויין כי דרך זיהוי הנגיף היא ע"י זיהוי מחרוזת (STRING) מסוימת, שינוי המחרוזת לא יאפשר גילוי הנגיף. התוכנה אינה יעילה, כדי להפעילה על המשתמש לעבור מספר מסכים דבר המסרבל את העבודה.

SBEXTERM

תוכנה המיועדת אך ורק לטיפול בנגיף הפינג-פונג. התוכנה אינה מונעת אותה אלא רק "מנקה" את הדיסקט.

JIV21

התוכנה מטפלת בנגיפים הנדבקים למקטע התיחול (BOOT SECTOR). מטפלת נגיפים פינג-פונג, פקיסטני ונגיף השגיאות.

UNVIRUS של יובל רכבי

UNVIRUS 6.0

התוכנה מזהה ומנקה נגיפים אך אינה מחסנת בפני נגיפים. תהליך ניקוי הנגיפים אמין יותר משאר תוכנות PUBLIC DOMAIN. הנגיפים בהם התוכנה מסוגלת לטפל הינם:

הנגיף הישראלי, פינג-פונג, פקיסטני, שגיאות, והראשון באפריל.

יצויין כי אין אלו הנגיפים המצויים בארץ, כמו כן התוכנה אינה מגינה בפני כל הגירסאות של הנגיפים, למרות זאת תוכנה זו הינה אמינה והיא הטובה ביותר מתוך תוכניות PUBLIC DOMAIN.

UNVIRUS 5.5

גירסא זו מכילה מספר תוכניות:

IMMUNE - מונעת הרצת תוכנית נגועה בנגיף. התוכנה בודקת פסיקה (INT21) ולכן אינה יעילה כנגד רוב סוגי הנגיפים. בתוכנות מסוימות יכולה להיווצר בעיה בזמן הפעלתם.

UNVIRUS5.5 - מחסלת וירוסים מתוך קבצים.

CHKVIRUS - תוכנית זו בודקת את הזכרון (RAM) של המחשב להימצאות נגיף. במקרה ויש נגיף בזכרון תצא הודעה על הימצאות נגיף והוא ינוטרל.

TIMERUN - מאפשר להריץ תוכנית כעבור פרק זמן מסוים ללא התערבות המשתמש.

IMMUNE25

תוכנה פותחה בממר"מ על ידי רפי שיפמן זוהי תוכנה היושבת בזכרון המחשב (RESIDENT), התוכנה אמורה למנוע מנגיף להכנס לזכרון ולהתפשט בשאר המחשב. התוכנה אינה יעילה כנגד כל נגיפי המחשב הקיימים בארץ. הגירסה האחרונה היא V.5, בקרוב צפוייה להתפרסם גירסה חדשה.

תוכנות ההגנה למחשבי מקינטוש

חברת "APPLE" משווקת מספר תוכנות הגנה כנגד נגיפים. את התוכנות האלו ניתן לחלק לשלוש קבוצות:

1. תוכנות איתור נגיפים כגון VIRUS CHECK ,VIRUSDETECTIVE, VIRUS RX ו-INTERFERON. תוכנות אלו מאתרות את נגיפי הניקוד (SCORES) וה-NVIR גם יחד. קיימות תוכנות FERRET ו- KILL SCORES יעודית לחיפוש SCORES בלבד. כמובן קיימת תוכנית ייעודית REZSEARCH לנגיף ה-NVIR.
2. תוכנות דו-שימושיות, המקובלות גם בארץ, שתפקידן איתור והשמדת הנגיפים. התוכנות הן:
   א. תוכנה "נגד נגיפית" UNVIR 2.0.
   ב. תוכנת "טיהור" DISINFECT.
3. תוכנית התראה וחיסון מפני פגיעה נגיפית - תוכנית "התרכיב" VACCINE.

המסמך מטפל אך ורק בתוכנות הקיימות והשימושיות בארץ, דהיינו בתוכנת UNVIR 2.0, "טיהור" ו-"תרכיב". הדרך המהירה והיעילה לחיפוש נגיף "הניקוד" (SCORES) היא לפתוח את תיק המערכת (SYSTEM FOLDER). ואם במקום צלם(ציור גראפי) של מקינטוש (ICON) המופיע עבור קבצי הארכיון (SCRAPBOOK) וקבצי דף הנתונים (NOTEPAD) יופיעו צלמי (ICONS) דף עם אוזניים (דף מקופל בקצה) יש להניח בוודאות כי המערכת נגועה. אם לא מתגלה נגיף, יש להתקין את תוכנת התרכיב (VACCINE) בתיק המערכת (SYSTEM FOLDER). כאשר תוכנית ויראלית כלשהי מנסה לשנות פרטים, תוכנית "התרכיב" תציג מערכת דו שיח ותשאל את המשתמש האם הוא מעוניין להמשיך בתוכנית המקורית למרות העובדה שקיים חשש סביר לנגיף או לא.
התשובה צריכה להיות - לא! וזאת ע"י הקלדת המילה DENIED. מייד אחר כך יש להריץ תוכנה נגד-נגיפית כלשהי (דוגמא UNVIR2.0 או DISINFECT).

לפני הרצת תוכנית "התרכיב" יש לנקוט במספר צעדי זהירות כדלקמן:

א. הרץ תוכנית איתור נגיף בטרם התקנת תוכנית התרכיב. מאחר ואם המערכת כבר נגועה בנגיף, כל תהליך "דו-שיח" אינו מתבצע. דבר זה עלול לגרום למערכת ליפול או להיתקע.

ב. ישנם דיווחים, כי שילוב תוכנת התרכיב עם מערכת הפעלה SYSTEM 6.0 הסבה נזק בצורת נפילות ושינויים הרסניים בקבצי INIT וה-CDEV.

המסמך הוכן בעזרתו של -
סמ"ר חיים כוריאל - בהתנדבות!